

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

SCOTT HEARD, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ATLAS OIL COMPANY,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Scott Heard, individually and on behalf of all others similarly situated, brings this action against Atlas Oil Company (“Atlas”). The following allegations are based on Plaintiff’s knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Atlas responsible for the injuries Atlas inflicted on Plaintiff and approximately 500 similarly situated persons (“Class Members”) due to Atlas’s impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the “Data Breach” or “Breach”) on May 5, 2024.¹

¹ *Atlas Oil: The Consequences of a Ransomware Attack*, Trustwave (June 25, 2024), <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/atlas-oil-the-consequences-of-a-ransomware-attack/>

2. The data that Atlas caused to be exfiltrated by cybercriminals were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information (“PII”) like full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, payroll information, passports, driver’s licenses, and “other identifying information.”²

3. Subsequently, the Black Basta cybercriminal group took credit for the Data Breach.³

4. Upon information and belief, prior to and through the date of the Data Breach, Atlas obtained Plaintiff’s and Class Members’ PII and then maintained that sensitive data in a negligent and/or reckless manner.

5. As evidenced by the Data Breach, Atlas inadequately maintained its information technology systems—rendering these easy prey for cybercriminals—and failed to adequately train its employees against “phishing” and other social engineering attacks.

6. Upon information and belief, the risk of the Data Breach was known to Atlas, especially given the known high frequency of cyberattacks and data breaches targeting employers in possession of PII. Thus, Atlas was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

² *Id.*

³ *Id.*

7. Moreover, Atlas failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, Atlas deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Even when Atlas finally notified Plaintiff and Class Members of the exfiltration of their PII, Atlas failed to adequately describe the Data Breach and its effects.

8. Simply put, Atlas impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

9. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of Atlas’s negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

10. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members’ names, take out loans using Class Members’ identities, use Class Members’ names to obtain medical services, use Class Members’ identities to obtain government benefits, file fraudulent tax returns using Class Members’ information, obtain driver’s licenses in Class Members’ names (but with another person’s photograph), and give false information to police during an arrest.

11. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach. Furthermore, Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Through this action, Plaintiff seeks to remedy these injuries individually and on behalf of all similarly situated individuals whose PII were exfiltrated and compromised in the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Atlas’s data security systems and employee cybersecurity training, future annual audits, and adequate identity and credit monitoring services funded by Atlas.

PARTIES

14. Plaintiff Heard is a natural person and resident of Harris County, Texas. He has no intention of moving to a different state in the immediate future.

15. Defendant Atlas Oil Company is a Michigan-based oil company, with its principal place of business in Oakland County, Michigan.

JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. And minimal diversity is established because many members of the Class are citizens of states different than that of Atlas.

17. This Court has general personal jurisdiction over Atlas because Atlas's principal place of business and headquarters is in this District. Atlas also regularly conducts substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Atlas conducts substantial business in this District.

FACTUAL ALLEGATIONS

Atlas Collected and Stored the PII of Plaintiff and Class Members

19. Atlas is a company that offers fuel distribution services, delivering over 1 billion gallons of fuel every year to customers across 49 states of the United States.⁴

⁴ *About Us*, Atlas Oil, <https://www.atlasoil.com/about-us/> (last accessed July 8, 2024).

20. Upon information and belief, Atlas received and maintained the PII of its current and former employees. These records are stored on Atlas's computer systems.

21. Upon information and belief, Atlas's computer systems were targeted via phishing and ransomware attacks, resulting in the Breach and the exfiltration of Plaintiff's and Class Members' PII.

22. Because of the highly sensitive and personal nature of the information Atlas acquires and stores, Atlas knew or reasonably should have known that it stored protected PII and must comply with data security industry standards and all federal and state laws protecting current and former employees' PII and provide adequate notice to individuals if their PII is disclosed without proper authorization.

23. When Atlas collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

24. Atlas acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

25. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, Atlas assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

26. On Atlas's Privacy Policy, published on its website, Atlas represents that, "[t]he security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security."⁵

27. Upon information and belief, Atlas represented to the public, including Plaintiff and Class Members, that it would properly protect all PII it obtained.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

29. Upon information and belief, Plaintiff and Class Members relied on Atlas to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Atlas could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

⁵ *Privacy Policy*, Atlas Oil (Mar. 1, 2024), <https://www.atlasoil.com/privacy-policy/>

31. Atlas's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

32. Despite the prevalence of public announcements of data breaches and data security compromises, Atlas failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

33. Atlas failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

34. Atlas failed to ensure the proper monitoring and logging of file access and modifications.

35. Atlas failed to ensure the proper training of its and its technology partners' employees as to cybersecurity best practices.

36. Atlas failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

37. Atlas failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

38. Atlas knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

39. Atlas failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and potentially disclose it to others without consent.

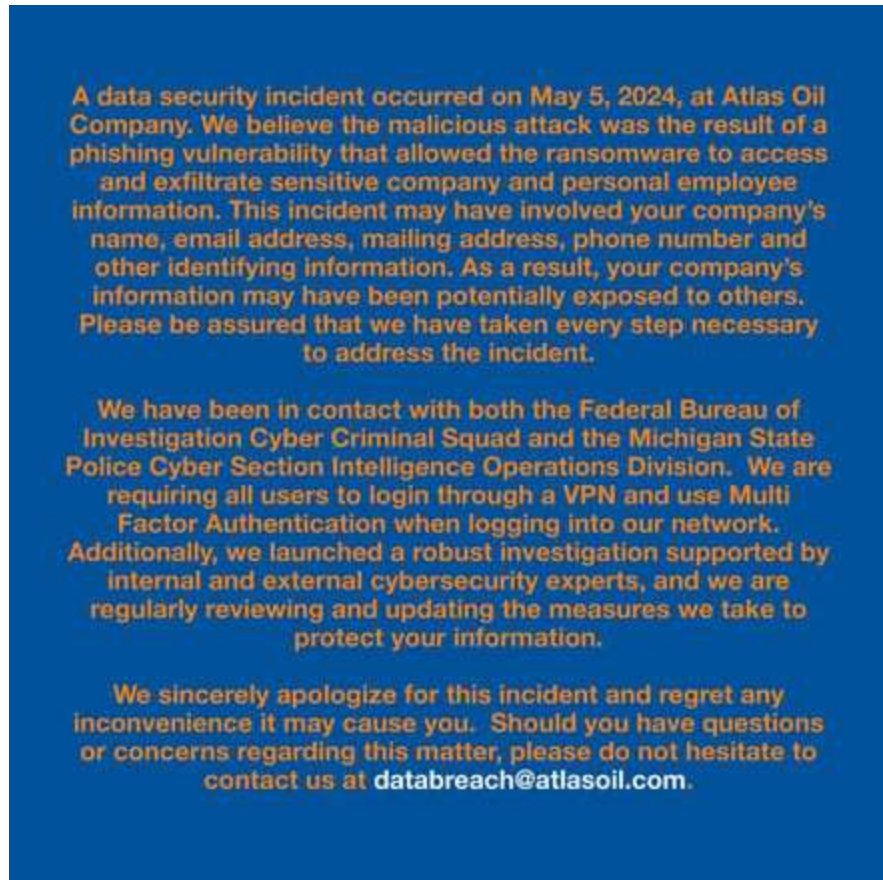
40. Upon information and belief, Atlas failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

41. Upon information and belief, Atlas failed to ensure the proper encryption of Plaintiff's and Class Members' PII and monitor user behavior and activity to identify possible threats.

The Data Breach

42. On or about June 2024, Atlas posted on its website a notice ("Data Breach Notice" or "Notice"), stating that employee personal information had been compromised in a Data Breach suffered by Atlas.

43. The online Notice is accessible by going to Atlas's official website and clicking on a link at the top of the website reading, "For information regarding the recent data breach, click here." The link then takes users to a JPEG image file, posted below:



Atlas's official response to the Data Breach

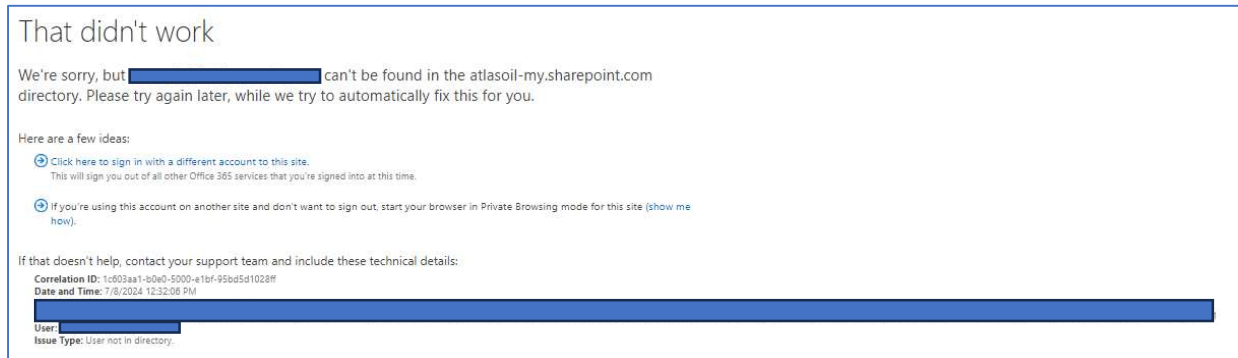
44. Upon information and belief, Atlas posted the Notice on its webpage as a hyperlinked JPEG image file to preclude search engines from indexing the content and to downplay coverage of the Data Breach.⁷

45. As of the filing date of the instant Class Action Complaint, whenever an Internet user clicks on the top of Atlas's webpage reading, "For information regarding the recent data breach, click here", the user is directed to log into an Atlas

⁶ *Atlas Oil: The Consequences of a Ransomware Attack*, Trustwave (June 25, 2024), <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/atlas-oil-the-consequences-of-a-ransomware-attack/>

⁷ *Id.*

SharePoint site and enter an email address in order to access Atlas's information on the Data Breach. Only users with email addresses recognized by Atlas's SharePoint directory are permitted access to Atlas's information about the Data Breach.



Screenshot of the error message displayed when a user attempts to authenticate with Atlas's SharePoint website to access information about the Data Breach

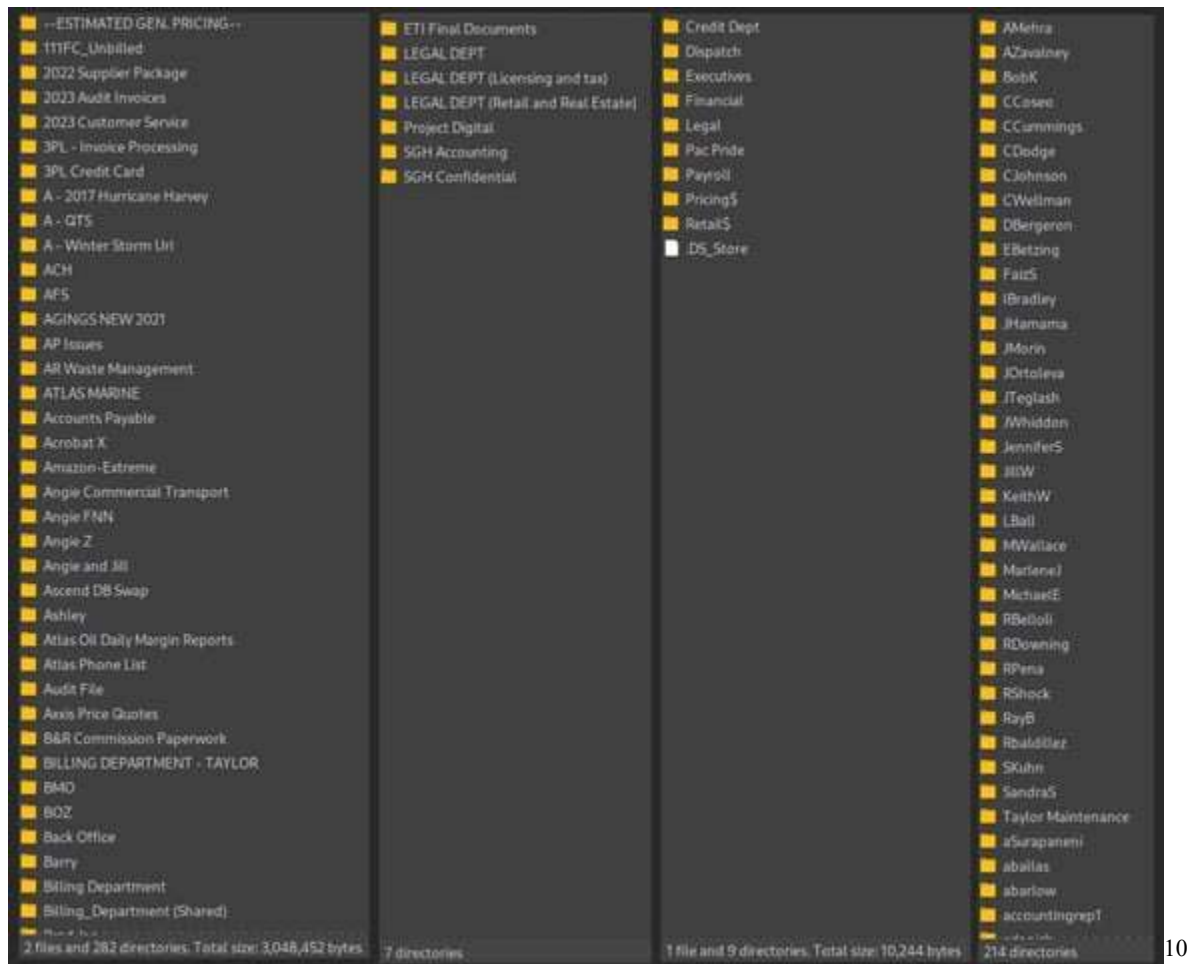
46. Upon information and belief, Atlas imposed (and continues to impose) authentication and authorization requirements to access information about the Data Breach in order to hinder concerned individuals from discovering information about the incident.

47. Upon information and belief, the Black Basta cybercrime group claimed responsibility for the Data Breach.⁸

48. As “proof” of responsibility for the Data Breach, Black Basta posted on its ‘dark web’ site a screenshot of a file directory structure of Atlas’s internal files and documents, those of which were downloaded by Black Basta. The screenshot

⁸ *Id.*

indicates that sensitive business data, including financial records, customer service data, and employee-related files, may have been compromised.⁹



Screenshot of the folders claiming to have been downloaded by Black Basta

49. On its dark web page, Black Basta also posted screenshots showing collections of—among other things—IDs, passports, driver's licenses, notarized

⁹ *Id.*

¹⁰ *Id.*

documents containing private information, scanned documents with payroll information, and birth certificates.¹¹

50. Upon information and belief, Atlas has sufficient control over its data.

51. Upon information and belief, Plaintiff's and Class Members' affected PII was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

52. It is likely the Data Breach was targeted at Atlas due to its status as large oil company that collects, creates, and maintains PII.

53. Atlas was unreasonably delayed in providing notice of the Breach to Plaintiff and Class Members.

54. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

¹¹ *Id.*

55. Atlas largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

56. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.¹²

57. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;¹³ leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"¹⁴ Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

¹² *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS <https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour> (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make \$1,253 per 40-hour work week.).

¹³ Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC <https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html> (Nov. 6, 2019).

¹⁴ *Id.*

58. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

59. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

60. Atlas also offered identity theft monitoring services for a period of 12 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

61. Atlas had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

62. Atlas's Notice letter, as well as its difficult-to-access website notice, both omit the size and scope of the Breach.

63. Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what

steps are being taken, if any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Atlas intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

64. Plaintiff's and Class Members' PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

Data Breaches Are Preventable

65. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

66. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

67. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.¹⁵ In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.¹⁶ Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.¹⁷ In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.¹⁸

68. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for

¹⁵ *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/>

¹⁶ *Ransomware FAQs*, available at <https://www.cisa.gov/stopransomware/ransomware-faqs>

¹⁷ *Ponemon study finds link between ransomware, increased mortality rate*, available at <https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate>

¹⁸ *The State of Ransomware in Healthcare 2022*, available at <https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf>

additional revenue.”¹⁹ As cybersecurity expert Emisoft warns, “[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence [...] the initial assumption should be that data may have been exfiltrated.”

69. An increasingly prevalent form of ransomware attack is the “encryption+exfiltration” attack in which the attacker encrypts a network and exfiltrates the data contained within.²⁰ In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.²¹ Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be “assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt.”²² And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.²³

¹⁹ *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>

²⁰ *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>

²¹ 2020 Ransomware Marketplace Report, available at <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

²² *Id.*

²³ *Id.*

70. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”²⁴

71. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless

²⁴ How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²⁵

72. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

²⁵ *Id.* at 3-4.

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²⁶

²⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

73. Given that Defendant was storing the PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

74. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the PII of approximately five hundred individuals, including that of Plaintiff and Class Members.

Atlas Failed to Comply with FTC Guidelines

75. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making.²⁷ To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Atlas, should employ to protect against the unlawful exfiltration of PII.

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.²⁸ The guidelines explain that businesses should:

²⁷ *Start with Security: A Guide for Business*, FED. TRADE COMM’N (June 2015), <https://bit.ly/3uSoYWF> (last accessed July 25, 2022).

²⁸ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM’N (Oct. 2016), <https://bit.ly/3u9mzre> (last accessed July 25, 2022).

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

77. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

78. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.²⁹

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

²⁹ See *Start with Security*, *supra* note 46.

these actions further clarify the measures businesses must take to meet their data security obligations.

80. Atlas's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Atlas Failed to Follow Industry Standards

81. Despite its alleged commitments to securing sensitive data, Atlas does not follow industry standard practices in securing PII.

82. Experts studying cyber security routinely identify large companies, such as Atlas, as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

83. Several best practices have been identified that at a minimum should be implemented by companies like Atlas, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

84. Other best standard cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network

systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

85. Atlas failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness. Such frameworks are the existing and applicable industry standards in Atlas's industry. And Atlas failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiff and Class Members

86. Plaintiff and Class Members are current and/or former employees of Atlas.

87. As a prerequisite of receiving employment, Atlas requires its employees—like Plaintiff and Class Members—to hand over their PII.

88. When Atlas finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Atlas's Breach Notice fails to explain how the Breach occurred, what exact data elements

of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

89. Because of the Data Breach, Atlas inflicted injuries upon Plaintiff and Class Members. And yet, Atlas has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

90. All Class Members were injured when Atlas caused their PII to be exfiltrated by cybercriminals.

91. Plaintiff and Class Members entrusted their PII to Atlas. Thus, Plaintiff and Class Members had the reasonable expectation and understanding that Atlas would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff and Class Members would not have entrusted their PII to Atlas had they known that Atlas would not take reasonable steps to safeguard their information.

92. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Atlas obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

93. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

94. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Scott Heard's Experience

95. Plaintiff Scott Heard was an Atlas employee until 2019.

96. Plaintiff Heard first learned of the Breach when he received a notice via mail from Defendant on June 4, 2024, which informed him that his PII had been compromised in the Breach.

97. Shortly after and as a result of the Data Breach, Plaintiff Heard experienced a significant increase in spam communications, including email, text, and phone calls.

98. As a result of the Data Breach, Plaintiff Heard was notified that a credit card was opened using his PII compromised from the Data Breach. Plaintiff has since been able to get the fraudulent credit card account closed.

99. As a result of the Data Breach, Plaintiff Heard made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to reviewing financial statements and reviewing his credit.

100. Plaintiff Heard has spent over six (6) hours responding to the Data Breach, the time spent of which included searching for fraudulent charges and researching events surrounding the Data Breach. Plaintiff will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

101. Plaintiff Heard suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and/or financial information.

102. Plaintiff Heard is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties/criminals.

103. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Atlas's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

104. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to Atlas.

105. The ramifications of Atlas's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information, such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

106. According to experts, one out of four data breach notification recipients become a victim of identity fraud.³⁰

107. As a result of Atlas's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;

³⁰ *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/>.

- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in the possession of Atlas and is subject to further breaches so long as Atlas fails to undertake the appropriate measures to protect the PII in their possession.

108. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.³¹

³¹ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

109. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

110. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

111. One such example of criminals using PII for profit is the development of "Fullz" packages.³²

112. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

³² "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) <https://krebsonsecurity.com/tag/fullz/>.

113. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and other members of the proposed Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

114. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.

115. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.” Atlas did not rapidly report to Plaintiff and the Class that their PII had been stolen.

116. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

117. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

118. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

119. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information

collected by businesses, or why their information may be commercially valuable.

Data is currency.”³³

120. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.³⁴ According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.³⁵

121. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers’ finances, credit history and reputation, and can take time,

³³ *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

³⁴ *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Oct. 21, 2022).

³⁵ *Id.*

money, and patience to resolve the fallout.³⁶ The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the “FTCA”).

122. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Atlas] allowed users to bypass authentication procedures” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) (“[Atlas] failed to employ sufficient measures to detect unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) (“[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s Inc.*, No. C-4291 (May 20, 2010) (“[Atlas]

³⁶ *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen>.

failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization” and “failed to use readily available security measures to limit access between instore networks . . .”). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Atlas thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

123. Charged with handling highly sensitive PII, Atlas knew or should have known the importance of safeguarding the PII that was entrusted to it. Atlas also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Atlas’s former and current employees as a result of a breach. Atlas nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

124. Atlas disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Atlas opened, disclosed, and failed to adequately protect the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts,

and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

125. Atlas's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

126. Atlas's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

128. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

All persons residing in the United States whose PII was impacted by the Data Breach—including all persons that received a Data Breach Notice (the “Class”).

129. The Class defined above is readily ascertainable from information in Atlas’s possession. Thus, such identification of Class Members will be reliable and administratively feasible.

130. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Atlas, Atlas’s subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Atlas or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff’s counsel and Atlas’s counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

131. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

132. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

133. **Numerosity.** The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at

this time, based on information and belief, the Class consists of hundreds of individuals whose PII was compromised by Atlas's Data Breach.

134. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

- a. If Atlas unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. If Atlas failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. If Atlas's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. If Atlas's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. If Atlas owed a duty to Class Members to safeguard their PII;
- f. If Atlas breached its duty to Class Members to safeguard their PII;

- g. If Atlas knew or should have known that its data security systems and monitoring processes were deficient;
- h. If Atlas should have discovered the Data Breach earlier;
- i. If Atlas took reasonable measures to determine the extent of the Data Breach after it was discovered;
- j. If Atlas's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;
- k. If Atlas's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;
- l. If Atlas's conduct was negligent;
- m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;
- n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Atlas's misconduct;
- o. If Atlas breached implied contracts with Plaintiff and Class Members;
- p. If Atlas was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;
- q. If Atlas failed to provide notice of the Data Breach in a timely manner; and

- r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

135. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Atlas's uniformly illegal and impermissible conduct.

136. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

137. **Predominance**. Atlas has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same information technology systems and unlawfully and inadequately protected in the same way. The common issues arising from Atlas's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

138. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common

questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Atlas. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

139. The litigation of the claims brought herein is manageable. Atlas's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

140. Adequate notice can be given to Class Members directly using information maintained in Atlas's records.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 123.

142. Atlas has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

143. Plaintiff re-alleges and incorporates by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

144. Atlas required Plaintiff and Class Members to submit their non-public PII to Atlas to be considered for and obtain employment with Atlas.

145. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Atlas owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Atlas's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

146. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Atlas holds vast amounts of PII, it was

inevitable that unauthorized individuals would at some point try to access Atlas's databases of PII.

147. After all, PII is highly valuable, and Atlas knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Atlas knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

148. Atlas owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

149. Atlas's duty of care to use reasonable security measures arose because of the special relationship that existed between Atlas and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Atlas was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

150. Atlas failed to take appropriate measures to protect the PII of Plaintiff and the Class. Atlas is morally culpable, given the prominence of security breaches in Atlas's industry. Any purported safeguards that Atlas had in place were wholly inadequate.

151. Atlas breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in Atlas's industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII.

152. The failure of Atlas to comply with industry and federal regulations evinces Atlas's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

153. But for Atlas's wrongful and negligent breach of their duties to Plaintiff and the Classes, Plaintiff's and Class Members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Atlas's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Classes and all resulting damages.

154. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Atlas's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Atlas knew or should have known that their systems and technologies for processing and securing the PII of Plaintiff and the Classes had security vulnerabilities.

155. As a result of this misconduct by Atlas, the PII and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater

risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Classes.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

156. Plaintiff re-alleges and incorporates by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

157. Under the Federal Trade Commission Act, Atlas had a duty to employ reasonable security measures. Specifically, this statute prohibits “unfair . . . practices in or affecting commerce,” including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.³⁷

158. Moreover, Plaintiff’s and Class Members’ injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Atlas inflicted upon Plaintiff and Class Members.

159. Atlas’s duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Atlas is bound by industry standards to protect confidential PII.

³⁷ 15 U.S.C. § 45.

160. Atlas owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Atlas also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Atlas's Data Breach.

161. Atlas owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Atlas knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Atlas actively sought and obtained the PII of Plaintiff and Class Members.

162. Atlas breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. And but for Atlas's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Atlas include, but are not limited to:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

- b. Failing to comply with—and thus violating—FTCA and its regulations;
- c. Failing to adequately monitor the security of its networks and systems;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Class Members' PII;
- f. Failing to detect in a timely manner that Class Members' PII had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

163. It was foreseeable that Atlas's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Atlas's industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

164. Simply put, Atlas's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper

disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Atlas's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

165. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Atlas to, *e.g.*, (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

168. This claim is pleaded in the alternative to the breach of implied contract claim below.

169. Plaintiff and Class Members conferred a monetary benefit on Atlas, by paying money for services, a portion of which was intended to have been used by Atlas for data security measures to secure Plaintiff and Class Members' PII. Plaintiff

and Class Members further conferred a benefit on Atlas by entrusting their PII to Atlas from which Atlas derived profits.

170. Atlas enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Atlas instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Atlas's failure to provide adequate security.

171. Under the principles of equity and good conscience, Atlas should not be permitted to retain the money belonging to Plaintiff and Class Members, because Atlas failed to implement appropriate data management and security measures that are mandated by industry standards.

172. Atlas acquired the monetary benefit and PII through inequitable means in that Atlas failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

173. If Plaintiff and Class Members knew that Atlas had not secured their PII, they would not have agreed to give their money—or disclosed their data—to Atlas or Atlas's customers.

174. Plaintiff and Class Members have no adequate remedy at law.

175. As a direct and proximate result of Atlas's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII, which remain in Atlas's possession and is subject to further unauthorized disclosures so long as Atlas fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Atlas's Data Breach.

176. As a direct and proximate result of Atlas's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

177. Atlas should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

178. Plaintiff re-alleges and incorporates by reference paragraphs 1-142 of the Complaint as if fully set forth herein.

179. Defendant required Plaintiff and the Class to provide and entrust their PII as a condition of being considered for and obtaining employment from Atlas.

180. Plaintiff and the Class provided their PII to Atlas in exchange for being considered for and obtaining employment, as well as Atlas's promises to protect their PII from unauthorized disclosure.

181. Through its course of conduct, Atlas, Plaintiff, and Class Members entered into implied contracts for Atlas to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

182. Atlas solicited and invited Plaintiff and Class Members to provide their PII as part of Atlas's regular business practices. Plaintiff and Class Members accepted Atlas's offers and provided their PII to Atlas.

183. As a condition of being former and/or current employees of Atlas, Plaintiff and Class Members provided and entrusted their PII to Atlas. In so doing, Plaintiff and Class Members entered into implied contracts with Atlas by which Atlas agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

184. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Atlas, in exchange for, amongst other things, the protection of their PII.

185. Plaintiff and Class Members fully performed their obligations under the implied contracts with Atlas.

186. Atlas breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

187. Atlas further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide with applicable laws and regulations.

188. Atlas's failures to meet these promises constitute breaches of the implied contracts.

189. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Atlas providing goods and services to Plaintiff and Class Members that were of a diminished value.

190. As a direct and proximate result of Atlas's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud,

and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

191. As a result of Atlas's breach of implied contract, Plaintiff and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

- A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;
- B. A mandatory injunction directing Atlas to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:
 - i. prohibiting Atlas from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Atlas to protect, including through encryption, all data collected through the course of business in accordance with

all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Atlas to delete and purge the PII of Plaintiff and Class Members unless Atlas can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Atlas to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;
- v. requiring Atlas to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Atlas's systems on a periodic basis;
- vi. prohibiting Atlas from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;
- vii. requiring Atlas to segment data by creating firewalls and access controls so that, if one area of Atlas's network is

compromised, hackers cannot gain access to other portions of Atlas's systems;

- viii. requiring Atlas to conduct regular database scanning and securing checks;
- ix. requiring Atlas to monitor ingress and egress of all network traffic;
- x. requiring Atlas to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;
- xi. requiring Atlas to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Atlas's policies, programs, and systems for protecting personal identifying information;
- xii. requiring Atlas to implement, maintain, review, and revise as necessary a threat management program to appropriately

monitor Atlas's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Atlas to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

- C. A mandatory injunction requiring that Atlas provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;
- D. Enjoining Atlas from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;
- F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;
- H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

- I. For all other Orders, findings, and determinations identified and sought in this Complaint; and
- J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: July 11, 2024

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 West Monroe Street, Suite 2100

Chicago, Illinois 60606

T: (866) 252-0878

gklinger@milberg.com

Jean S. Martin*

MORGAN & MORGAN

COMPLEX LITIGATION GROUP

201 North Franklin Street 7th Floor

Tampa, Florida 33602

T: (813) 559-4908

F: (813) 222-4795

jeanmartin@forthepeople.com

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class